SEC565: **Red Team Operations and Adversary Emulation**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Consume threat intelligence and plan a Red Team engagement
- Set up the required infrastructure to have a successful operation taking into account operational security
- Create weaponization that will allow you to infiltrate an organization
- Enumerate and extract valuable data required to achieve your objectives using automated tooling, but also manually, if required
- Move laterally and persist in a corporate network
- Elevate privileges using a variety of attack vectors and misconfigurations that you will now be able to identify
- Report your findings in a meaningful way to bring maximum value to your client

Prerequisites

The concepts and exercises in this course are built on the fundamentals of offensive security. An understanding of general penetration testing concepts and tools is encouraged, and a background in security fundamentals will provide a solid foundation upon which to build Red Team concepts.

Many of the Red Team concepts taught in this course are suitable for anyone in the security community. Both technical staff as well as management personnel will be able to gain a deeper understanding of Red Team exercises and adversary emulations.

Penetration testing is effective at enumerating vulnerabilities, but less effective in addressing personnel and processes on the defense side. This can leave Blue Teams or defenders without sufficient knowledge of what offensive input to improve, in turn leaving organizations stuck in a cyclical process of just focusing on vulnerabilities in systems rather than on maturing defenders to effectively detect and respond to attacks.

In SEC565, students will learn how to plan and execute end-to-end Red Teaming engagements that leverage adversary emulation, including the skills to organize a Red Team, consume threat intelligence to map against adversary tactics, techniques, and procedures (TTPs), emulate those TTPs, report and analyze the results of the Red Team engagement, and ultimately improve the overall security posture of the organization. As part of the course, students will perform an adversary emulation against a target organization modeled on an enterprise environment, including Active Directory, intelligence-rich emails, file servers, and endpoints running in Windows and Linux.

SEC565 features six intensive course sections. We will start by consuming cyber threat intelligence to identify and document an adversary that has the intent, opportunity, and capability to attack the target organization. Using this strong threat intelligence and proper planning, students will follow the Unified Kill Chain and multiple TTPs mapped to MITRE® ATT&CK™(Adversarial Tactics, Techniques, and Common Knowledge) during execution. During three course sections, students will be immersed in deeply technical Red Team tradecraft ranging from establishing resilient and advanced attack infrastructure to abusing Active Directory. After gaining initial access, students will thoroughly analyze each system, pilfer technical data and target intelligence, and then move laterally, escalating privileges, laying down persistence, and collecting and exfiltrating critically impactful sensitive data. The course concludes with an exercise analyzing the Blue Team response, reporting, and remediation planning and retesting.

In SEC565, you will learn how to show the value that Red Teaming and adversary emulations bring to an organization. The main job of a Red Team is to make a Blue Team better. Offense informs defense and defense informs offense. SEC565 develops Red Team operators capable of planning and executing consistent and repeatable engagements that are focused on training and on measuring the effectiveness of the people, processes, and technology used to defend environments.

You Will Learn How To:

Use threat intelligence to study adversaries for emulation

Build an adversary emulation plan

Map actions to MITRE® ATT&CK™ to aid in communicating with the Blue Team

Establish resilient, advanced C2 infrastructure

Maintain operational security throughout an engagement

Leverage initial access to elevate and propagate through a network

Enumerate and attack Active Directory

Collect and exfiltrate sensitive data in a safe manner

Close an engagement, deliver value, and plan for retesting

Section Descriptions

SECTION 1: Planning Adversary Emulation and Threat Intelligence

During the first section of the course, we will present a common language to discuss adversary tactics and techniques. We will discuss the purpose of the Red Team and highlight the various frameworks and methodologies around this topic. Two critical steps before a successful adversary emulation are to conduct threat intelligence and to plan for the engagement. The section closes by looking at the first few actions during the Red Team engagement.

TOPICS: Adversary Emulation; Ethical Hacking Maturity Model; Frameworks and Methodologies; Understanding Adversaries; Unified Kill Chain; MITRE® ATT&CK™; Threat Intelligence; Threat Report ATT&CK™ Mapping (TRAM); ATT&CK™ Navigator; End-To-End Testing Model; Assumed Breach; Execution Phase; Building a Red Team – Skill Development; Reconnaissance; Open-Source Intelligence (OSINT); Password Attacks; Social Engineering; Attacks Against MFA – evilnginx2

SECTION 3: Getting In and Staying In

In the third section of the course, we will prepare our malicious payloads through weaponization. We will discuss various methods of delivery in order to achieve that initial access into the target network. After surveying the initial host and surrounding network, we will stealthily propagate through the network in a cycle of discovery, privilege escalation, credential access, and persistence.

TOPICS: Weaponization; Custom Executables; Blending In; Execution Guardrails; Initial Access; Network Propagation; Discovery; Operational Security; Deception Technology; Local Network Enumeration; Local Privilege Escalation; Password Cracking; Persistence

SECTION 5: Obtaining the Objective and Reporting

In section five, we will use our newly exploited access to discover critical and sensitive information stored in the environment. We will collect and exfiltrate these data and demonstrate the impact of the Red Team s actions. After the active testing period, the Red Team must analyze the engagement, deliver reporting, and plan for retesting. The section will close with preparations for the immersive Red Team Capture-the-Flag Exercise in the final course section.

TOPICS: Action on Objectives; Database Attacks; SQL Abuse; Trust Abuse; PowerupSQL; Target Manipulation; Collection; Data Staging; Exfiltration; Impact; Emulating Ransomware; Engagement Closure; Analysis and Response; Red Team Reveal; Measuring People and Processes; Retesting; Remediation and Action Plan; Breach and Attack Simulation; APTSimulator; Network Flight Simulator; Atomic Red Team; MITRE® CALDERA; SCYTHE

SECTION 2: Attack Infrastructure and Operational Security

The second section of the course will introduce various Red Team tools and command-and-control frameworks, both of which rely on a well-maintained attack infrastructure. We will spend most of the section discussing the important aspects of a resilient attack infrastructure and how the Red Team can create a bit of distance from defenders by utilizing redirectors. Another key aspect of protecting the attack infrastructure that will be discussed is implementing monitoring and operational security.

TOPICS: Red Team Tools; Command and Control (C2); C2 Comparison; Listeners and Communication Channels; Advanced Infrastructure; Redirectors; Third-Party Hosting; Comparison of Self-Hosted vs. Third-Party; Operational Security; Understand IoCs; Introduction to VECTR; Covenant

SECTION 4: Active Directory Attacks and Lateral Movement

The fourth course section dives deep into Microsoft Active Directory (AD), learning and practicing the tactics, techniques, and procedures used to attack and enumerate it. We will use various tools to enumerate, escalate, and pivot through these enterprise networks, including Domain and Forest Trusts, and identify how we can move between them.

TOPICS: Introduction to Active Directory; Trees and Forests; Authentication, Authorization, Access Tokens; AD Enumerate; DNS Extraction; Domain Privilege Escalation; Access Token Manipulation; Pass-The-Hash, Pass-The-Ticket; Kerberoasting; Silver Ticket, Golden Ticket, Skeleton Key; AD Certificate Services; Unconstrained and Constrained Delegation; Coerced Authentication Using PrinterBug and PetitPotam; Hopping the Trust; LLMNR/NBNS/WPAD; Bloodhound/SharpHound; AD Explorer; SMB Pipes, Remote Desktop Protocol, PsExec, Windows Management Instrumentation, dcom; SMB Relay; LLMNR/NBT-NS Poisoning and Relay; Responder; Setting Up Shadow Credentials; Domain Privilege Abuse; DC Sync; Domain Lateral Movement, Domain Trust Attacks; Pivoting Between Domains and Forests; Forest Enumeration, Forest Attacks

SECTION 6: Immersive Red Team Capture-the-Flag

In section six, we will conduct a Red Team engagement in a threat representative range depicting a Windows Active Directory enterprise network. Students will each have their own environment consisting of three domains. This story driven environment provides ample opportunity for each student to exercise many of the skills learned throughout the course. The environment is seasoned with rich user stories, target intelligence, and user activity. We will target Windows servers, workstations, and databases along with Active Directory infrastructure. We will also attack Linux servers and databases leveraging the systems maneuver through the segmented network.

TOPICS: Adversary Emulation; Reconnaissance; Initial Access; Persistence and Privilege Escalation; Credential Access; Discovery; Lateral Movement; Collection; Command and Control; Exfiltration; Impact; Closure

Who Should Attend

- Security professionals interested in expanding their knowledge of Red Team engagements in order to understand how they are different from other types of security testing
- Penetration testers and Red Team members looking to better understand their craft
- Blue Team members, defenders, and forensic specialists looking to better understand how Red Team engagements can improve their ability to defend by better understanding offensive methodologies, tools, tactics, techniques, and procedures
- Auditors who need to build deeper technical skills and/or meet regulatory requirements
- Information security managers who need to incorporate or participate in high-value Red Team engagements

Authors' Statement

"Organizations are maturing their security testing programs to include Red Team engagements and adversary emulations. These engagements provide a holistic view of an organization's security posture by emulating a realistic adversary to test security assumptions, measure the effectiveness of people, processes, and technology, and improve detection and prevention controls. This course will teach you how to plan Red Team engagements, leverage threat intelligence to map against adversary tactics, techniques, and procedures, build a Red Team program and plan, execute a Red Team engagement with a strong emphasis on operational security and tradecraft, and report and analyze the results. Direct application of the lessons in this course will give Red Team operators the skills necessary to improve the overall security posture of an organization."
—Barrett Darnell

"With this course we provide students with a blueprint they can use to set up a realistic Red Team operation against a client environment. Students will be able to consume threat intelligence, formulate a plan of attack, execute it, and ultimately create a debrief package that will provide maximum value for their organization. This course truly brings together a wide variety of knowledge and aims to equip the students with state-of-the-art tradecraft, keeping up to date with the latest and greatest TTPs. No other course brings together such a wide variety of knowledge of all things Red Team."
—Jean-Françis Maes